Bijlage bij de brief aan de minister van Binnenlandse Zaken en Koninkrijksrelaties

Inhoudsopgave

Bijlagen:

- Vragen die zijn gesteld aan verschillende experts ten aanzien van het beveiligingsniveau en Common Criteria certificering
- Uitwerking van de controle van elektronisch getelde stembiljetten

1. Beveiligingsniveau: stelsel van Common Criteria en EAL-niveaus

De commissie heeft zich voor de beantwoording van de nadere vragen van de minister van BZK nader verdiept in het stelsel van de Common Criteria (CC). In dat kader hebben leden van de commissie gesproken met deskundigen op dit terrein. De vragen die aan deze deskundigen zijn gesteld en de antwoorden die zijn ontvangen zijn aan dit document gehecht. Eveneens is aan dit document gehecht een beschrijving op hoofdlijnen van het CC-stelsel.

Dilemma's

Om misbruik van de stemprinter en stemmenteller te voorkomen wordt door de commissie een combinatie van technische maatregelen en procedures voorgesteld die het mogelijk zou moeten maken om misbruik te voorkomen dan wel om misbruik te detecteren.

De maatregelen die gericht zijn op de detectie zullen, als de detectie werkt (en het systeem dus doet wat het moet doen), zichtbaar maken dat er misbruik is gepleegd of dat er een vermoeden daarvan bestaat. Als dat gebeurt tijdens een verkiezing of na een verkiezing dan zal dat tot de nodige commotie leiden. Immers onmiddellijk is dan de vraag aan de orde of de stemprinter en/of stemmenteller nog vertrouwd kunnen worden. Vindt de detectie voorafgaand aan de verkiezing plaats dan kan, mits daarvoor een wettelijke grondslag bestaat, de verkiezing worden uitgesteld. Dat zal evenwel ook heel wat consequenties kunnen hebben.

De goede werking van het voorgestelde concept (techniek + procedure), waarvan detectie van misbruik of het vermoeden daarvan een essentieel kenmerk is, leidt derhalve tot een hogere kans op significante (politieke) problemen bij de organisatie van de verkiezingen. In het verleden, ten tijde dat de stemmachines in gebruik waren, was dat risico er niet of veel kleiner omdat maatregelen om misbruik te detecteren ontbraken. Er waren immers alleen functionele eisen voor de stemmachines vastgesteld.

Gelet op de voorgeschiedenis van het dossier elektronisch stemmen, maar ook de in algemene zin kritische opstelling in Nederland ten aanzien van de beveiliging van ICT-systemen, mag verwacht worden dat allerlei (capabele) personen en groeperingen gemotiveerd zullen zijn om de robuustheid van de stemprinter en stemmenteller onder de loep te nemen en om te proberen om aan te tonen dat deze systemen niet goed beveiligd zijn. De hogere complexiteit van het concept van de stemprinter en stemmenteller ten opzichte van het huidige proces met het papieren stembiljet dat handmatig wordt geteld, leidt tot een grotere kans op dergelijke aanvallen (waarbij het doel van de aanval niet een succesvolle manipulatie van het kiesproces is, maar een succesvolle poging van de manipulatie van het systeem). Zouden dergelijke aanvallen slagen dan is de vraag hoe lang het vertrouwen in de stemprinter en/of stemmenteller in stand kan blijven.

Concluderend zou kunnen worden gesteld dat een hoog niveau van (openbaar gemaakte) gedocumenteerde beveiliging van de stemprinter en stemmenteller deze motivatie om de hiervoor genoemde aanvallen uit te voeren kan reduceren waardoor de kans op commotie en verminderd vertrouwen afneemt.

Wat zijn de Common Criteria (CC)

De Common Criteria [CC] vormen een instrument voor het evalueren en beoordelen van de informatiebeveiliging van ICT-producten en –systemen. Voor het beoordelen wordt gebruik gemaakt van de documentatie van de ICT-producten en het ICT-systeem. Tevens worden testen op de ICT-producten en het ICT–systeem uitgevoerd.

De CC zijn het resultaat van inspanningen van deskundigen om criteria voor evaluatie van ICT-beveiling te ontwikkelen die gebruikt zouden kunnen worden in internationaal verband. Aan de CC liggen meerdere reeds ontwikkelde criteria ten grondslag zoals bestaande Europese, Amerikaanse en Canadese criteria (respectievelijk ITSEC, TCSEC en CTCPEC).

De structuur van CC biedt flexibiliteit bij het specificeren van beveiligde ICT-producten en -systemen. Opdrachtgevers, leveranciers en andere partijen kunnen de beveiligingsfunctionaliteit van een ICT-product en ICT-systemen specificeren in een beschermingsprofiel en het niveau voor de evaluatie bepalen, gebruikmakend van een gedefinieerde set van zeven oplopende EAL's (Evaluation Assurance Levels), van EAL1 t/m EAL7.

Bij het definiëren van de beveiliging moeten allereerst de dreigingen worden geïnventariseerd waartegen de ICT-producten en -systemen beschermd moeten worden. De CC bevat een catalogus aan eisen die kunnen worden gebruikt om het gewenste beveiligingsniveau te realiseren. Met gebruikmaking van deze catalogus wordt het zogenaamde Protection Profile (PP) opgesteld. Bij het opstellen van het PP wordt systematisch vastgesteld of voor elke geïdentificeerde dreiging afdoende maatregelen getroffen kunnen worden. De specifieke invulling van de maatregelen wordt uitgeschreven in het Security Target (ST).

EAL-niveaus[1]

De CC bevat een reeks gedefinieerde niveaus. Om te voldoen aan specifieke doelstellingen, kan een niveau worden uitgebreid met één of meerdere aanvullende onderdelen uit een hoger niveau (de zogenaamde "plus"). Om ervoor te zorgen dat systemen voldoen aan de vereisten van deze niveaus, moeten ze zijn ontworpen en ontwikkeld met de intentie om aan die vereisten te voldoen.

EAL1 is het instapniveau. Tot EAL-niveau 4 worden de vereisten strenger en meer gedetailleerd, maar worden geen zeer gespecialiseerde technieken op het gebied van beveiligingsengineering vereist. EAL1-4 kunnen over het algemeen worden gebruikt voor de modificatie van reeds bestaande producten en systemen. Boven niveau EAL4 wordt een toenemende mate van toepassing vereist van gespecialiseerde technieken op het gebied van beveiligingsengineering.

Evaluatie en certificering

De evaluatie bestaat uit een beoordeling van de vereiste documentatie over en van de ICT-producten en het ICT-systeem en uit testen die de evaluator uitvoert. De evaluator moet geaccrediteerd zijn bij een van de instanties die bevoegd zijn om te certificeren.

---

[1] Zie voor nadere informatie de website van het Common Criteria Portal, waar een meer uitgebreide beschrijving staat van de zeven EAL-niveaus. Zie daarvoor het volgende document: http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf (hoofdstuk 8).

De evaluator controleert dat de documentatie over het ICT-product en –systemen aan de CC-vereisten voldoet. De evaluator beoordeelt, als dat volgt uit het betreffende EAL-niveau, de testrapportages van de ontwikkelaar. Daarbij wordt nagegaan of de uitgevoerde testen dekkend zijn. Hier past wel een kanttekening. Volgens de CC moet de ontwikkelaar alleen in functionele zin de beveiliging testen. Penetratietesten hoeft de ontwikkelaar zelf niet te doen. Penetratietesten worden door de evaluator uitgevoerd. Pas als de ontwikkeling van het systeem is afgerond start de evaluator met de testen. De evaluator moet aan de certificerende instantie vooraf voorleggen welke testen er zullen worden uitgevoerd. De certifcerende instantie beoordeelt of die testen, voor het betreffende EAL-niveau dekkend zijn.

Hieronder wordt, op grote hoofdlijnen, weergegeven welke testen de evaluator uitvoert. De intensiviteit, zowel wat betreft de middelen als wat betreft de tijdsduur, verschilt per EAL-niveau. Hoe hoger het niveau, hoe intensiever en diepgaand de testen worden uitgevoerd en hoe langer ze duren.

EAL-niveau	Wat test de evaluator	Afgedekt dreigingniveau/attack potential vlgs CC
1	De gebruikersfuncties worden getest voor zover de evaluator die belangrijk vindt voor de beveiliging. Voert penetratietesten uit uitsluitend om na te gaan of het te evalueren product cq systeem bestand is tegen op internet gepubliceerde kwetsbaarheden.	Dreigingniveau: Basaal/Basic EAL 1 tot en met 3 bieden bescherming tegen de kennis en mogelijkheden van personen die geen specifieke vaardigheden of kennis bezitten en zich alleen richten op algemeen bekende kwetsbaarheden, of in aanvulling daarop willekeurige pogingen doen om kwetsbaarheden te vinden. Als het gaat om internettechnologie vallen bijv. de zgn. "script-kiddies" in deze categorie, ofwel personen die gebruik maken van gepubliceerde hulpmiddelen voor de aanval op kwetsbaarheden zonder deze kwetsbaarheden noodzakelijkerwijs te begrijpen.
2 en 3	Beveiliginggerelateerde gebruikersfuncties worden getest. Dezelfde penetratietesten worden uitgevoerd als bij EAL 1. Naast de gepubliceerde kwetsbaarheden wordt ook getest op kwetsbaarheden die de evaluator heeft geïdentificeerd bij het beoordelen van de documentatie die de leverancier levert van het product cq systeem.	Dreigingniveau: Basaal/Basic Idem als bij EAL 1.
4	Gebruikersfuncties worden getest. Dezelfde penetratietesten worden uitgevoerd als bij EAL 1 t/m 3. Daarenboven wordt ook getest op kwetsbaarheden die de evaluator heeft geïdentificeerd bij de beoordeling van de broncode van het product cq systeem.	Dreigingniveau: Hoger dan basaal/Enhanced basic EAL 4 biedt bescherming tegen de kennis en mogelijkheden van personen die beschikken over IT-vaardigheden op een bepaald technologisch gebied, maar niet gespecialiseerd zijn in het zoeken naar kwetsbaarheden.

EAL-niveau	Wat test de evaluator	Afgedekt dreigingniveau vlgs CC
5	Gebruikersfuncties worden getest. Dezelfde penetratietesten worden uitgevoerd als bij EAL 1 t/m 4. Omdat bij dit niveau er veel meer gedetailleerde documentatie moet worden gemaakt van het product cq systeem heeft de evaluator ook veel meer kennis omtrent het systeem en de mogelijke kwetsbaarheden daarvan waarop dan ook getest wordt.	Dreigingniveau: Matig/Moderate EAL 5 biedt bescherming tegen de kennis en mogelijkheden van beveiligingsexperts (door leken "hackers" genoemd, hoewel sommige "hackers" mogelijk een hoger deskundigheidsniveau hebben).
6	Zie EAL 5. Bij EAL 6 geldt dat het product cq systeem met gebruikmaking van semi-formele methoden moet zijn ontworpen en ontwikkeld, met uitzondering van belangrijke aspecten van de beveiliging en de relatie daarvan met het gedrag van het product cq systeem. Die aspecten moeten met gebruikmaking van formele methoden zijn ontworpen en ontwikkeld. Waar gebruik is gemaakt van formele methoden biedt dat de mogelijkheid om op wiskundige wijze de correcte werking vast te stellen.	Dreigingsniveau: Hoog/High EAL 6 biedt bescherming tegen de kennis en mogelijkheden van een civiel beveiligingslab of een georganiseerde groep hackers of een universitair team gespecialiseerd in de technologie die wordt gebruikt in het product.

De evaluator zal, gerelateerd aan het EAL-niveau van de certificering, uiteraard steeds proberen om bij het testen na te gaan of het systeem bestand is tegen de meest actuele dreigingen die hij kan vinden. Mede daardoor bestaat het risico dat bij de testen door de evaluator een kwetsbaarheid in het systeem wordt ontdekt. In dat geval zal de leverancier aanpassingen moeten verrichten aan het systeem om de kwetsbaarheid weg te nemen. Dit risico bestaat overigens ook als er voor gekozen wordt geen CC-certificering uit te laten voeren. Het is namelijk ondenkbaar dat de opdrachtgever (in casu de overheid) in het kader van de acceptatie van de systemen geen beveiligingstesten, waaronder penetratietesten, laat uitvoeren.

De certificering zelf geschiedt door de instanties die bevoegd zijn tot het afgeven van het certificaat. Het resultaat is een certificaat waarin het bereikte waarborgingsniveau van de beoordeling (EAL) wordt vermeld en een bijbehorend certificeringsrapport waarin een samenvatting wordt gegeven van de uitkomst van de certificering.

2. Nadere uitwerking van de methode voor de controle van de elektronisch getelde stembiljetten

In haar rapport heeft de commissie geadviseerd om steekproefsgewijs een deel van de elektronisch getelde papieren stembiljetten te controleren. Dit is een van de fundamenten onder het concept van de commissie waarin het papieren proces leidend is. Voor de beantwoording van de nadere vragen heeft de commissie door professor dr. E.C. Wit van de Rijksuniversiteit Groningen

aanvullend werk laten verrichten aan de methode die zou kunnen worden gebruikt voor deze controle. Het rapport van professor Wit is als bijlage bij dit document gevoegd. Een centraal element van de methode is de risicomarge die gehanteerd moet worden. Het hanteren van een risicomarge is nodig omdat er fouten bij het elektronisch tellen, net al bij handmatig tellen, niet kunnen worden uitgesloten. Het rapport van professor Wit bevat de bouwstenen om te kunnen bepalen welke marge er voor de controle aangehouden kan worden. Hoe kleiner de marge hoe meer stembiljetten er gecontroleerd moeten worden.

3. Aantal stemprinters per stemlokaal

In haar rapport is de commissie van het volgende uitgegaan:

- 10.000 stembureaus en gemiddeld 1.000 kiezers per stembureau;
- Eén stemprinter per stembureau en 2.500 reserve stemprinters voor het geval op de dag van de verkiezing een stemprinter als gevolg van gebreken moet worden vervangen;
- Bij meervoudige verkiezingen wordt op 1 stembiljet de keuze voor 1 verkiezing geprint.

De commissie heeft in haar rapport onderkend dat bij meervoudige verkiezingen mogelijk niet zou kunnen worden volstaan met 1 stemprinter per stemlokaal. Gezien de beperkte tijd die beschikbaar was voor de werkzaamheden van de commissie en de complexiteit van het vraagstuk is aan deze constatering verder geen uitwerking gegeven.

Naar aanleiding van de nadere vragen die de minister van BZK heeft gesteld, is alsnog verder onderzocht hoeveel stemprinters daadwerkelijk nodig zouden kunnen zijn per stemlokaal. Het is duidelijk dat meervoudige verkiezingen een feit zijn. In ieder geval zullen de verkiezingen van provinciale staten en de besturen van de waterschappen in de toekomst (te beginnen in 2015) op 1 dag plaatsvinden. Daarnaast moet er rekening mee worden gehouden dat in de toekomst op 1 dag mogelijk meerdere raadgevende referenda worden gehouden dan wel een of meerdere referenda in combinatie met een (andere) verkiezing.

Voor het onderzoek is gebruik gemaakt van de tijdmetingen die het ministerie van BZK heeft laten uitvoeren bij testen in 2012 en tijdens de herindelingverkiezingen op 19 november 2014. Deze tijdmetingen laten zien dat een kiezer gemiddeld 30 seconden bezig is om het huidige stembiljet in te vullen en dat de leden van de stembureaus er gemiddeld 30 seconden over doen om de kiezer te voorzien van zijn/haar stembiljet.

Verder is gebruik gemaakt van gegevens van de gemeente Rotterdam over de tijdstippen waarop kiezers hun stem hebben uitgebracht bij de verkiezing voor de gemeenteraad in maart 2014. Hieruit is op te maken dat ca 30% van de kiezers in de laatste drie uur (dus tussen 18.00 en 21.00 uur) hun stem uitbrengen.

<u>Scenario's</u>

De stemprinter die de commissie voor ogen heeft is nog niet uitgespecificeerd. Er zijn daarbij nog vele keuzes te maken, bijvoorbeeld met betrekking tot de wijze van activering, maar ook ten aanzien van de interface die zal worden ontwikkeld om de kiezer een keuze te laten maken en het stembiljet te printen. Er zijn verder geen referentiegegevens beschikbaar van een stemprinter in andere landen. Zouden die er zijn, dan is het overigens maar de vraag in hoeverre die gegevens bruikbaar zouden kunnen zijn, gelet op de verschillen die er bestaan tussen landen ten aanzien van het kiesstelsel.

Om toch een inschatting te kunnen maken van het aantal noodzakelijke stemprinters heeft de commissie een drietal scenario's opgesteld. Voor deze scenario's gelden de volgende uitgangspunten:

- De scenario's gaan uit van meervoudige verkiezingen, te weten van 3 verkiezingen die tegelijk plaatsvinden (twee lijstverkiezingen en een (landelijk) raadplegend referendum).

- De kiezer activeert zelf de stemprinter. Dit is overeenkomstig het rapport van de commissie. In de navolgende berekening is ervan uitgegaan dat de kiezer één token per verkiezing meekrijgt. Daarom is een keer 5 seconden geschat voor het activeren.

- Er wordt geen rekening mee gehouden dat een deel van de kiezers (tussen de 10 à 15% van de kiezers) ook 1 of 2 volmachtstemmen uitbrengt. Aangenomen mag worden dat het (mede) uitbrengen van een volmachtstem minder tijd in beslag neemt dan het uitbrengen van een eigen stem. Deze tijdswinst zal naar schatting echter beperkt blijven tot 10 à 20% per volmachtstem. Dit resulteert in 1-3% tijdwinst over het geheel. Dit is voor dit moment te verwaarlozen.

- Er wordt geen rekening mee gehouden dat sommige kiezers audio-ondersteuning nodig zullen hebben om de stemprinter te gebruiken. Er is geen inschatting te maken van het aantal kiezers dat deze ondersteuning nodig zal hebben.

- De kiezer kiest zelf de volgorde van de twee verkiezingen en het referendum.
- Het aantal interactieve stappen per verkiezing is minimaal.

- Tijd tussen opdracht tot printen en daadwerkelijk printen alsook de tijdsduur van het printen zelf zijn minimaal.

- Voor elke verkiezing wordt een afzonderlijk stembiljet aangemaakt.

- Het stembiljet wordt geprint na iedere keuze.

- Controleren van het stembiljet gebeurt door de kiezer bij de stemprinter, dus in het stemhokje.

De drie scenario's worden aangeduid met:

a. Minimaal;
b. Nominaal;
c. Maximaal.

Deze scenario's representeren een bandbreedte, waarbij de variatie met name bepaald wordt door de menselijke handelingen. Dat wil zeggen dat de technische aspecten (activeren, printen) in elk van de scenario's gelijk is, maar de handelingen die de kiezer verricht variëren.

Handeling	**Minimaal** tijd (sec)	**Nominaal** tijd (sec)	**Maximaal** tijd (sec)
Stemhokje binnengaan	2,5	2,5	2,5
Activeren	5	5	5
Keuze lijstverkiezing 1	15	20	25
Print lijstverkiezing 1	5	5	5
Controleren lijstverkiezing 1	5	7,5	10
Keuze lijstverkiezing 2	15	20	25
Print lijstverkiezing 2	5	5	5
Controleren lijstverkiezing 2	5	7,5	10
Keuze referendum	2,5	5	7,5
Print referendum	5	5	5
Controleren referendum	2,5	5	7,5
Stemhokje uitgaan	2,5	2,5	2,5
Totaal aantal seconden	70	90	110

<u>Berekening aantal stemprinters per stemlokaal</u>

Voor de berekening van het aantal stemprinters worden de volgende uitgangspunten gehanteerd:

a. De capaciteitsbehoefte (aantal verkiezingen, belangstelling) kan per verkiezing variëren, maar het aantal stemprinters moet toereikend zijn voor de piek. Dit betekent dat bij bepaalde verkiezingen sprake kan zijn van overcapaciteit, aangezien het aantal stemprinters zich niet per verkiezing laat bepalen. Deze worden voor een bepaalde periode waarin verschillende verkiezingen (met verschillende behoeften) plaatsvinden, verworven.

b. De spreiding over de dag is niet gelijk, met pieken tijdens het eerste openingsuur en de laatste drie uren van de dag. De capaciteit moet toereikend zijn voor deze pieken, met dien verstande dat de wachttijden niet langer zouden mogen moeten zijn dan men nu gewend is (en kennelijk niet tot problemen leidt). Op grond van metingen door gemeente Rotterdam wordt ervan uitgegaan dat tijdens piekuren 10% van de kiezers de stem uitbrengt, dus 100 per uur.

In onderstaand overzicht is de volgende berekening gemaakt:

a. Hoeveel kiezers kunnen in een uur met gebruikmaking van de stemprinter hun stem uitbrengen.
b. De capaciteitsbehoefte gegeven de piek (10% van de kiezers).
c. Hoeveel stemprintercapaciteit is nodig (b delen door a).
d. Benodigd aantal stemprinters.

	Minimaal	Nominaal	Maximaal
Aantal kiezers per uur	51	40	33
Benodigde piek capaciteit	100	100	100
Aantal stemprinters op piek	1,9	2,5	3,1
Benodigd aantal stemprinters	2	3	3

4. Kosten

De commissie heeft in haar rapport al opgemerkt dat er te veel onzekerheden zijn om de kosten van de invoering en het gebruik van de stemprinter en stemmenteller precies te kunnen ramen. Daarom is in het rapport een ruime marge aangehouden voor zowel de investeringskosten als voor de meerkosten per verkiezing.

Bij het beantwoorden van de nadere vragen heeft de commissie er kennis van genomen dat er kostenposten zijn die niet zijn meegenomen in de ramingen. In de tijd die beschikbaar was voor het beantwoorden van de nadere vragen was het niet mogelijk om zinvol nader onderzoek te doen om de ramingen te corrigeren. Overigens is het maar de vraag of, als er wel meer tijd zou zijn geweest, een dergelijk onderzoek bruikbare resultaten zou hebben opgeleverd. Er zijn namelijk te veel onzekere factoren, onder meer omdat er nog op vele onderdelen keuzes moeten worden gemaakt en verder gespecificeerd.